## REMARKS/ARGUMENTS

1. The Applicant has carefully considered the official communication dated September 21, 2007. Applicant respectfully submits that the amendment and the following remarks are fully responsive to the official communication.

2. The claims have been amended in light of the official communication. It is submitted that no new matter has been added as a result of the amendment.

3. In paragraph 1 of the Detailed Action, the Examiner alleges that claim 1 is not supported by US 09/516,874 (now granted as US 6,745,331). We respectfully submit that the present claims are adequately supported by 09/516,874 which shares a substantially common detailed description and figures to the present application.

4. We submit that claim 1 of the present application defines the invention described in detail, for example, with reference to "protocol 4" shown in Figure 6 (see line 55 of col.29 to line 40 of col. 31 in US 6,745,331). The authentication procedure of claim 1 includes the feature of a message authentication code (MAC) (see line 60 of col. 9 to line 20 of col. 10 in US 6,745,331) which is a construction of a cryptographic function (see second paragraph of col. 5 in US 6,745,331). Protocol 4 is a particular example of the authentication procedure defined by claim 1. Accordingly, we respectfully request that the Examiner recognize the priority claim.

5. We note the Examiner's submission that the present application cannot claim priority from an application filed in Australia on 15 July 1997. However, US 6,745,331 is a continuation of US 6,442,525, which claims priority from Australian Provisional Patent Application no. PO7991, filed on 15 July 1997. Accordingly, we respectfully submit that the present application is entitled to a priority date of 15 July 1997.

6. In paragraph 4 of the Detailed Action, the Examiner alleges that the detailed description does not disclose exactly how the authentication works. We respectfully submit that the skilled person would readily be able to implement authentication protocol 4 shown in Figure 6 and described in detail in the specification (as explained above), particularly when the accompanying description of protocol 4 is read in the context of the preceding description (including that of protocols 1 to 3 shown in Figures 3 to 5 respectively). Similarly, the skilled person could readily implement authentication protocols 1 to 3 described in detail with reference to Figures 3 to 5 respectively.

7. In paragraph 6 of the Detailed Action, the Examiner alleges that claims 1 to 7 are anticipated by US 2004/0223011 (Adkins et. al.). We propose amending claim 1 to include the features of claim 6 to further distinguish the present invention from Adkins et. al. Claim 6 is related to protocol 4 described in the specification and shown in Figure 6. Claim 1 now sets out that the asymmetric cryptographic function employs a pair of keys (a public key and a private key) and uses the keys for decrypting different information during authentication. We respectfully submit that this feature is neither disclosed nor suggested in Adkins et. al.

8. Instead, Adkins et. al. discloses a method for authenticating a consumable using a symmetric cryptographic function. As explained in the ultimate portion of paragraph [0038], each MAC is associated with a respective secret (i.e. key) that is used to encrypt and decrypt information. Whilst multiple keys are used, the keys employed are secret which is in contrast to the present invention where only one of the keys is secret, and the other is public (i.e. not secret). Accordingly, we respectfully submit that claim 1 is not anticipated by Adkins et. al.

9. Furthermore, Adkins et. al. does not disclose or suggest that the public key is used to decrypt an encrypted random number generated by another integrated circuit of the apparatus and the secret key used to decrypt encrypted data stored in the memory space (i.e. of the first mentioned integrated circuit). Accordingly, we submit that claim 1 is further not anticipated by Adkins et. al.

10. Claim 5 sets out that the integrated circuit is configured to define a number of temporary registers and rotating counters to calculate an output word on an iterative basis. Whilst Adkins et. al. does disclose the use of a single and fixed re-circulating counter to generate a random portion of a pseudo-random identification number (PID), there is no disclosure of using a number of temporary registers and rotating counters. Advantageously, the numerous registers and counters can be used to perform the processor intensive hash function (which is calculated iteratively), and their temporary nature conserves the available memory of the integrated circuit. Accordingly, we submit that claim 5 is also not anticipated by Adkins et. al.

11. In paragraph 8 of the Official Action, the Examiner has initially rejected claims 1 and 7 as being unpatentable over Matyas et al (US 4,918,728) in view of Omori et al. (US 5,790,667). Claim 1 now includes the features of claim 6 which were not objected to in light of these documents. We concur with the Examiner that the features of claim 1, as amended, are patentable over Matyas et al in view of Omori et al.

12. In paragraph 8 of the Official Action, the Examiner further alleges that claims 1-7 are unpatentable over Omori et al in view of Scneider. Neither citation relates to the authentication of consumables, and we therefore submit that there is no reason why the skilled person would combine these citations to arrive at the claimed invention. Furthermore, neither document discloses nor suggests using an asymmetric cryptographic function whereby a public key is used to decrypt an encrypted random number generated by another integrated circuit of the apparatus and a secret key is used to decrypt encrypted data stored in the memory space. Accordingly, we respectfully submit that claim 1 is patentable in light of these citations.

13. In addition, neither Omori et al nor Scneider disclose an integrated circuit configured to define a number of temporary registers and rotating counters to calculate an output word on an iterative basis, as claimed in claim 5. Accordingly, we respectfully submit that claim 5 is patentable in light of these citations.

It is respectfully submitted that all of the Examiner's objections have been successfully traversed. Accordingly, it is submitted that the application is now in condition for allowance. Reconsideration and allowance of the application is courteously solicited.

Very respectfully,

Applicant/s: 

Kia Silverbrook

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762